UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,252	01/31/2002	Massimiliano Antonio Poletto	12221-012001	2792

26161 7590 06/08/2007

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
06/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/066,252	POLETTO ET AL.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25 and 27-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 and 27-34 are pending.

Examiner notes that the original presentation of the claims provided no claim 26.

2. In view of the appeal brief filed on 25 January 2007, PROSECUTION IS HEREBY REOPENED. A non-final office action is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Kambiz Zand.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1 recites the limitation "the provisioned monitor" in line 7. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> ((a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. **Claims 1, 5, 11, 24, 27 are rejected under 35 U.S.C. 102(a)** as being anticipated by Mansfield "Towards trapping wily intruders in the large."

5. **With regards to claim 1**, Mansfield teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link) and collect statistical information on packets that are sent between a network and the data center for a plurality of customers (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) by examining traffic as if the device was disposed on links that are

downstream from the links that the provisioned monitor is on (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site).

6. **With regards to claims 5**, Mansfield teaches the monitoring device being a data collector device (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites).

7. **With regards to claims 11,** Mansfield teaches a provisioned monitor placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving the data center on the selected links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link) and collect statistical information for a plurality of provisioned customers which are on links that are downstream from links that the provisioned monitor is on (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

8. **With regards to claim 24**, Mansfield teaches collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) and maintaining separate counter logs for each provisioned customer (Mansfield, page 6,

traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the links on which collecting occurs (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

9. **With regards to claim 27**, Mansfield teaches collecting occurs on a data collector that samples network packets (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) the data collector being disposed at a location that is at a large aggregation link in the network for the data center (Mansfield, Figure 6, probe monitors traffic entering network 1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 2-3, 7, 9-10, and 33 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Mansfield "Towards trapping wily intruders in the large" in view of Crosbie et al US PGPub 2002/0083343.

11. **With regards to claim 2,** Mansfield fails to teach the monitoring device being coupled to a control center through a dedicated private network. However, Crosbie teaches the monitoring device being coupled to a control center through a dedicated

private network (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).

12. **With regards to claim 3**, Mansfield as modified teaches a communication process that communicates statistics with the control center and which receives queries or instructions from the control center (Mansfield, page 6, NMS collects information from traffic monitors, page 10, agents can be accessed, queried, configured by security manager).

13. **With regards to claim 7**, Mansfield teaches collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site). Mansfield fails to teach the communicating data over a dedicated private network to a control center. However, Crosbie teaches the communicating data over a dedicated private network to a control center (Crosbie, paragraph 0116-0118, SSL connection between management station and agent

systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).

14. **With regards to claims 9**, Mansfield as modified teaches the monitoring device being a data collector device (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites).

15. **With regards to claim 10**, Mansfield teaches the collecting occurring for inbound and outbound traffic (Mansfield, page 8, looks for reply messages, page 9, looks for request messages, Figure 8, incoming and outgoing).

16. **With regards to claim 33,** Mansfield teaches the control center determines a response to the attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach communicating occurs on a downstream link basis over a dedicated, hardened network to a control center. However, Crosbie teaches communicating occurs on a downstream link basis over a dedicated, hardened network to a control center (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network

and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).

17. **Claims 4, 6, 12-15, 25, 28-32, and 34 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Mansfield "Towards trapping wily intruders in the large" in view of Kim US PGPub 2002/0069356.

18. **With regards to claim 4,** Mansfield teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

19. **With regards to claim 6**, Mansfield as modified teaches a process to aggregate traffic from the various links and to produce logs and detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

20. **With regards to claim 12,** Mansfield teaches the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link), but fails to teach the monitoring device is a

gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

21. **With regards to claim 13**, Mansfield as modified teaches a global counter log that accounts for all traffic (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

22. **With regards to claim 14**, Mansfield as modified teaches the global counter includes a sample of all traffic seen on the link to which the gateway is connected (Mansfield, page 9, NMS combines counts from probe 1 and probe 2 in Figure 8, Kim, Abstract, integrated security gateway).

23. **With regards to claim 15**, Mansfield as modified teaches packet analysis for a particular virtual monitor happens by classifying packets based on addresses at the time of analysis (Mansfield, pages 5-6, source of malicious packet is traced).

24. **With regards to claim 25,** Mansfield teaches data collecting (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), but fails to teach the monitoring device is a gateway device located at the edge of a network. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway) located at the edge of a network (Kim, Figure 4 Item 420). At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

25. **With regards to claim 28,** Mansfield teaches performing intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate malicious traffic (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

26. **With regards to claim 29**, Mansfield as modified teaches collecting statistical information for a plurality of links that are downstream from links on which collecting occurs (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4), performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4),

and communicating alerts that arise from the traffic analysis (Mansfield, pages 10-11, security manager is alerted to the detection of potential attempts).

27. **With regards to claim 30**, Mansfield as modified teaches the performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites).

28. **With regards to claim 31**, Mansfield as modified teaches communicating to a control center occurs on a downstream link basis (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).

29. **With regards to claim 32**, Mansfield as modified teaches communicating to a control center occurs on a downstream link basis Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8) and the control center determines a response to the attack (Mansfield, page 10, security manager uses network information to trap or track down intruder).

30. **With regards to claim 34,** Mansfield teaches filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links (Mansfield, page 10, security manager uses network information to trap or track down intruder).

31. **Claim 8 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Crosbie et al US PGPub

2002/0083343, as applied to claim 7 above, and in further view of Kim US PGPub 2002/0069356.

32. **With regards to claim 8,** Mansfield as modified teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).

33. **Claims 16 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Kim US PGPub 2002/0069356, as applied to claim 13 above, and in further view of Gales US PGPub 2003/0084323.

34. **With regards to claim 16**, Mansfield as modified fails to teach the gateway maintaining duplicate packets keeping both a global packet log and a packet log for each virtual monitor. However, Gales teaches the gateway maintaining duplicate packets keeping both a global packet log and a packet log for each virtual monitor (Gales, paragraph 0016, network activity log for information about global network

usage, paragraph 0018, activity profile data has information for each of the nodes including inbound and outbound communication data). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Gales' method of keeping duplicate logs because it offers the advantage of allowing determination of security events on both a network and particular node level (Gales, paragraphs 0021-0022).

35. **Claim 17 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Kim US PGPub 2002/0069356, as applied to claim 13 above, and in further view of Syvanne et al US Patent No. 7,162,737 and Gales US PGPub 2003/0084323.

36. **With regards to claim 17**, Mansfield as modified teaches a process to aggregate traffic from probes (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8) and to produce a global counter log and produce detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8, page 8, looks for reply messages, page 9, looks for request messages, Figure 8, incoming and outgoing) and a node head (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8). Mansfield as modified fails to teach producing a separate counter log for each provisioned customer or the gateway being a clustered gateway with a plurality of probes. However, Gales teaches the gateway maintaining packet log for each virtual monitor (Gales, paragraph 0016, network activity log for information about global network usage, paragraph 0018, activity profile data has

information for each of the nodes including inbound and outbound communication data). Syvanne teaches the gateway being a clustered gateway with a plurality of probes (Syvanne, column 5 line 60 – column 6 line 10, clustered gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Syvanne's cluster methodology and Gale's logging method because it offers the advantage of allowing determination of security events on both a network and particular node level (Gales, paragraphs 0021-0022) and allows the flexible and reliable synchronization of state information between nodes in a gateway cluster (Syvanne, column 4 lines 50-60).

Allowable Subject Matter

37. Claims 18-23 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

38. The following is a statement of reasons for the indication of allowable subject matter: The cited prior art fails to teach or suggest the provisioned monitor including a virtual monitor for the physical link on which the provisioned monitor is deployed is configured to be an independent node in the network capable of issuing attack warnings and responses to attack queries independently from the virtual monitors of the provisioned monitor. As a result, the cited prior art fails to anticipate or render obvious the above cited claims.

Conclusion

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571 273 8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

Zand
2134